

XEROX**RECEIVED
CENTRAL FAX CENTER****JUL 25 2005****FACSIMILE COVERSHEET****TO:****MAIL STOP APPEAL BRIEF-PATENTS**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Fax: 571-273-8300

TOTAL NUMBER OF PAGES (including cover sheet): 32**FROM:**

Daniel B. Curtis
Xerox Corporation
Palo Alto Research Center Incorporated
3333 Coyote Hill Road
Palo Alto, CA 94304
Tel.: 650-812-4281

RE:**CERTIFICATE OF TRANSMISSION**

I hereby certify that this correspondence is being facsimile
transmitted to the Patent and Trademark Office to
Fax No. 571-273-8300 on 7/25/2005.

Daniel B. Curtis

(Typed or printed name of person signing this certificate)

 (Signature)

Application No. : 09/596,924
Filed : 6/12/2000
Inventor(s) : Thomas A. Berson et al.
Docket No. : A0461-US-NP
Confirmation No. : 4488
Examiner : Aravind K. Moorthy
Art Unit : 2131
Title : SYSTEM, METHOD AND ARTICLE OF
MANUFACTURE FOR DETERMINING A PRICE OF
CRYPTOGRAPHIC SERVICES BASED ON A
COMPUTATIONAL BURDEN
Customer No. : 25453

IMPORTANT/CONFIDENTIAL: This message is intended only for the use of the individual or entity to which it is addressed. This message contains information from the Office of General Counsel of Xerox Corporation which may be privileged, confidential and exempt from disclosure under applicable law which is not waived due to misdelivery. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately at the telephone number set forth above. We will be happy to arrange for the return of this message via the United States Postal Services to us at no cost to you.

RECEIVED
CENTRAL FAX CENTER

JUL 25 2005

PATENT APPLICATION

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office to Fax No.: 571-273-8300 on 7/25/2005.

Typed or printed name of person signing this certificate

Daniel B. Curtis

Signature:



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application of: Thomas A. Berson et al.

Appl. No.: 09/596,924

Filed: 6/19/2000

) Art Unit: 2131

) Examiner: Aravind K. Moorthy

) Confirmation No.: 4488

**Title: SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR DETERMINING A
PRICE OF CRYPTOGRAPHIC SERVICES BASED ON A COMPUTATIONAL BURDEN**

TO THE COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appellant's Brief in the above-identified application.

- ☒ Charge \$500.00 to Deposit Account No. 24-0025.
- ☒ Please charge any additional fees under 37 C.F.R. §§1.16, 1.17 and 1.21 (but not 1.18) or credit any overpayment to Deposit Account No. 24-0025.
- ☒ This constitutes a request for any needed extension of time and an authorization to charge all fees therefor to the above deposit account, if not otherwise specifically requested.

Respectfully submitted,



Daniel B. Curtis
Attorney for Appellant
Registration No. 39,159
Telephone: 650-812-4259

Date: July 25, 2005

~~07/27/2005 TBESHAN 00000025 240025 09396924~~

~~01 FC:1402 -500.00 DA~~

PATENT APPLICATION

RECEIVED
CENTRAL FAX CENTER

JUL 25 2005

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND
INTERFERENCES**

In re the Application of: **Berson et al.**

Group Art Unit: **2131**

Application No.: **09/596,924**

Examiner: **ARAVIND K MOORTHY**

Filed: **06/19/2000**

Docket No.: **A0461-US-NP**

For: **SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR
DETERMINING A PRICE OF CRYPTOGRAPHIC SERVICES BASED ON A
COMPUTATIONAL BURDEN**

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Sir:

Appellant respectfully submits this Appeal Brief in the appeal of the above identified case to the Board of Appeals and Patent Interferences on the Notice dated 4/25/2005.

Appeal from Group 2131

XEROX Corporation



Daniel B. Curtis

Telephone: (650) 812-4259

Attorney for Appellants

07/27/2005 TBESHAH1 00000025 09596924
01 FC:1402 500.00 DA

Docket No.: A0461-US-NP

Application No.:09/569,924

TABLE OF CONTENTS

| | Page |
|---|------|
| I. Introduction..... | 1 |
| II. Real party in interest | 1 |
| III. Related appeals and interferences | 1 |
| IV. Status of claims | 2 |
| V. Status of amendments | 4 |
| VI. Summary of claimed subject matter..... | 5 |
| A. Independent claims 1, 8 and 15..... | 5 |
| B. Dependent claims 2, 9 and 16 | 6 |
| C. Dependent claims 3, 10 and 17 | 6 |
| D. Dependent claim 4, 11, and 18..... | 7 |
| E. Dependent claims 5, 12 and 19 | 7 |
| F. Dependent claims 6, 13 and 20 | 7 |
| G. Dependent claims 7, 14 and 21 | 7 |
| VII. Grounds of rejection to be reviewed on appeal..... | 8 |
| VIII. Argument | 9 |
| A. Whether claims 1, 2, 4, 5, 8, 9, 11, 12, 15, 16, 18 and 19 are properly rejected under 35 U.S.C. §102(e) as anticipated by Bhagavath et al (6,343,117 B1). | 9 |
| 1. Claims 1, 8 and 15 | 9 |
| 2. Claims 2, 9 and 16 | 12 |
| 3. Claims 4, 11 and 18 | 12 |
| 4. Claims 5, 12 and 19 | 12 |
| B. Whether claims 3, 10 and 17 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1 in view of Iwamura (6,272,535 B1). | 15 |

Docket No.: **A0461-US-NP**Application No.: **09/569,924**

| | | |
|-----|--|----|
| 1. | The asserted combination of references fails to teach the claimed invention..... | 16 |
| 2. | There is no motivation or suggestion in the prior art to make the asserted combination of references..... | 17 |
| C. | Whether claims 6, 13 and 20 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1 in view of Billstrom (5,729,537)..... | 18 |
| D. | Whether claims 7, 14 and 21 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1 in view of Jakobsson (6,049,613 B1). | 19 |
| IX. | Conclusion | 20 |
| X. | Claims APPENDIX | 21 |

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

I. Introduction

This is an appeal from a Final Office Action mailed 1/27/2005, finally rejecting claims 1-21 of the above-identified patent application.

II. Real party in interest

The real party in interest in this appeal in the present application is Xerox Corporation, by way of an assignment recorded at recl/frame 10932/0164.

III. Related appeals and interferences

There are presently no appeals or interferences, known to Applicant, Applicant's representative or the Assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Docket No.: A0461-US-NP

Application No.:09/569,924

IV. Status of claims

Claims 1-21 are pending in this application.

Pending claims 1-21 are finally rejected in the outstanding Office Action and are on appeal. Of the claims that are on appeal, claims 1 (a method claim), 8 (a computer program product claim) and 15 (a system claim) are independent claims. Claims 2-7 directly or indirectly depend from claim 1. Claims 9-14 depend from claim 8. Claims 16-21 directly or indirectly depend from claim 15. Claims 1- 24 are set forth in the attached Appendix.

Applicant hereby appeals the rejection of claims 1-21. Claims 22-24 have been previously canceled.

| Claim | Under Appeal Status | Rejected Status | Allowed Status | Withdrawn Status | Objected-to Status | Canceled Status |
|-------|---------------------|-----------------|----------------|------------------|--------------------|-----------------|
| 1 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 2 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 3 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 4 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 5 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 6 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 7 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 8 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 9 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 10 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 11 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 12 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 13 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 14 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |

Docket No.: A0461-US-NP

Application No.:09/569,924

| Claim | Under Appeal Status | Rejected Status | Allowed Status | Withdrawn Status | Objected-to Status | Canceled Status |
|-------|---------------------|-----------------|----------------|------------------|--------------------|-----------------|
| 15 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 16 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 17 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 18 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 19 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 20 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 21 | Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Not Canceled |
| 22 | Not Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Canceled |
| 23 | Not Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Canceled |
| 24 | Not Appealed | Rejected | Not Allowed | Not Withdrawn | Not Objected to | Canceled |

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

V. Status of amendments

No amendment after final rejection has been filed.

A Notice of Appeal was filed on 4/25/2005 in response to the final Office Action mailed on 1/27/2005. No amendments have been filed subsequent to the final rejection. This appeal brief was due on 6/25/05 but faxed to the United States Patent and Trademark office on 7/25/05. Thus, applicant petitions for a one month extension in accordance with 37 CFR 41.37(e) and 37 CFR 1.136(a)(1), and has authorized the fee specified in 37 CFR 1.17(a).

Docket No.: A0461-US-NP

Application No.:09/569,924

VI. Summary of claimed subject matter

A. Independent claims 1, 8 and 15

Claims 1, 8, and 15 are respectively directed to a method, computer program product, and system for pricing a "cryptographic service" on a network utilizing one or more cryptoservers.

A cryptoserver is located at a well connected node on a network and is configured to perform CPU intensive cryptographic computations. The cryptoserver may include special purpose hardware devices for performing the cryptographic computations (page 15, lines 19-26).

The claimed invention is directed towards determining the price of a **cryptographic service** that identifies the computational burden required to perform the cryptographic service. The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22.

To summarize, a cryptographic service provider operates a cryptographic server. The cryptographic server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the cryptographic server that provides the service of performing the cryptographic operation (page 20, lines 17-22). The client pays for the requested cryptographic service (page 19, lines 13-19; page 21, lines 1-5). One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a cryptographic server that determines the price of the requested service and performs the requested cryptographic service for the client.

The cryptographic service is thus a service provided by a cryptoserver that off-loads the computational burden due to cryptographic operations from a client computer. The pricing of this service is important as the operator of the client computer needs to be able to determine the cost of using the cryptographic service.

Docket No.: A0461-US-NP

Application No.:09/569,924

The price charged for the use of the cryptographic service can be based on the computational burden needed to perform the cryptographic service, the privacy level of the cryptographic service, or the speed of performing the cryptographic service. This is described in the instant application with regards to Fig. 7 starting at page 20, line 19 through page 22, line 2 and in particular to page 21 lines 22-30.

This summary of the invention discusses the claimed invention with reference to the elements of independent method claim 1. Since the elements of the system and computer program product claims are substantially similar to the elements of the method claim, the following summary of the claimed invention applies equally to the elements of the computer program product and system claims 8 and 15.

Original claim 1 is directed to a method for pricing a "cryptographic service" (page 20, lines 24-25; page 25, line 25 to page 27, line 2). The method receives a request for a cryptographic service, identifies a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing the cryptographic service, and determines a price of the cryptographic service based on the at least one of computational burden, privacy level, and speed (Fig. 7, page 20, line 29 through page 21, line 30).

B. Dependent claims 2, 9 and 16

Dependent claims 2, 9 and 16 limit their respective independent claims by having a user that is requesting the cryptographic service to specify the privacy level (original claim 2).

C. Dependent claims 3, 10 and 17

Dependent claims 3, 10 and 17 limit their respective independent claims by having a user that is requesting the cryptographic service to specify the speed of performing the cryptographic service (original claim 3).

Docket No.: A0461-US-NP

Application No.:09/569,924

D. Dependent claim 4, 11, and 18

Dependent claims 4, 11 and 18 limit their respective independent claims by requesting payment for the cryptographic service from a user that requested the cryptographic service. (original claim 4).

E. Dependent claims 5, 12 and 19

Dependent claims 5, 12 and 19 limit their respective independent claims by the cryptographic service utilizing private information retrieval (original claim 5).

F. Dependent claims 6, 13 and 20

Dependent claims 6, 13 and 20 limit their respective independent claims by the cryptographic service utilizing group authentication (original claim 6).

G. Dependent claims 7, 14 and 21

Dependent claims 7, 14 and 21 limit their respective independent claims by the cryptographic service utilizing mix networks (original claim 7).

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

VII. Grounds of rejection to be reviewed on appeal

- Whether claims 1, 2, 4, 5, 8, 9, 11, 12, 15, 16, 18 and 19 are properly rejected under 35 U.S.C. §102(e) as anticipated by Bhagavath et al (6,343,117 B1).
- Whether claims 3, 10 and 17 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1) in view of Iwamura (6,272,535 B1).
- Whether claims 6, 13 and 20 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1) in view of Billstrom (5,729,537).
- Whether claims 7, 14 and 21 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1) in view of Jakobsson (6,049,613 B1).

Docket No.: A0461-US-NP

Application No.:09/569,924

VIII. Argument

- A. Whether claims 1, 2, 4, 5, 8, 9, 11, 12, 15, 16, 18 and 19 are properly rejected under 35 U.S.C. §102(e) as anticipated by Bhagavath et al (6,343,117 B1).

1. Claims 1, 8 and 15

For a prior art reference to anticipate a claim, the reference must disclose each and every element of the claim with sufficient clarity to prove its existence in the prior art. *See In re Spada*, 911 F.2d 705, 708, 15 USPQ 2d 1655, 1657 (Fed. Cir. 1990) ([T]he [prior art] reference must describe the applicant's claimed invention sufficiently to have placed a person of ordinary skill in the field of the invention in possession of it. (citations omitted)). Although this disclosure requirement presupposes the knowledge of one skilled in the art of the claimed invention, that presumed knowledge does not grant a license to read into the prior art reference teachings that are not there. *Motorola, Inc. v. Interdigital Tech. Corp.*, 43 USPQ 2d 1481, 1490 (Fed. Cir. 1997)

One problem addressed by Bhagavath is that of securely providing VoIP over the Internet (Column 1, lines 42-46). The embodiment addressing this problem is related to Bhagavath Fig.

2. Bhagavath teaches a technology for encrypting VoIP data as it passes through the Internet. The caller is able to use DTMF (touch tones) to enable encryption of the conversation and to specify the level of encryption desired (Column 3, lines 55-59). Once the encryption is selected by the user, Bhagavath informs the user that encryption is enabled and optionally of the associated charges (Column 3, line 64-67) for providing the secure communication at the selected encryption level. The user can change the selected security level if desired (Column 4, lines 2-3).

Turning now to the invention of original claim 1 that is directed to a method for pricing a cryptographic service, comprising:

- (a) receiving a request for a cryptographic service;

Docket No.: A0461-US-NP

Application No.:09/569,924

- (b) identifying a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing the cryptographic service; and
- (c) determining a price of the cryptographic service based on the at least one of computational burden, privacy level, and speed.

Step (b) includes the limitation of identifying a computation burden for the requested service. As shown in step 720 of figure 7 the computational burden and/or the selected privacy level and/or the selected speed of performance is used to determine the price of the cryptographic service as per element (c) above.

While Bhagavath does teach pricing for encryption of VoIP data based on the desired privacy level, nothing in Bhagavath teaches step (b) of identifying a computational burden required to perform the cryptographic service. The office action did not provide a citation to Bhagavath supporting that assertion that a computational burden was identified by Bhagavath. While the Examiner did cite column 3 line 62 to column 4, line 3:

“Software controller 5 then instructs encryption/decryption module 8 to set up the appropriate level of security. Additionally, when the feature is activated, software controller 5 can initiate a verbal confirmation message informing the user that the feature is activated and optionally announce or display the associated charges. In the event that the user does not want to incur the charge associated with the selected security level, the user would have the option of selecting a cheaper alternative security level.”

nothing in the cited text or the application would teach one skilled in the art that the pricing for the selected security level has anything to do with the computational burden required to provide the selected security level. The pricing is for the value the user receives. All the user knows is cost to the user for the selected security level. The user does not make a decision based on the computational burden, but rather decides based on a cost/security level trade off. Applicant

Docket No.: A0461-US-NP

Application No.:09/569,924

asserts that price set by the provider is more likely to be market driven instead of related to the cost of providing the encryption.

In the "Response to Arguments" section of the final office action, the Examiner asserted that "the computational burden is based on the level of security the user chooses." While this is probably true, it is not relevant because pricing in Bhagavath appears to be value-oriented as is seen by Column 2, lines 28-39 where Bhagavath provides justification for higher prices based on the security level (also see Bhagavath's abstract). Thus:

"The invention enables telephone subscribers to select one of a plurality of security levels that may be required to ensure privacy during a call. Since each level of security is based on a different encryption and authentication algorithm, the levels of security can be incrementally priced. Accordingly, selecting an algorithm which is deemed to be very secure can be billed to the subscriber at a higher rate than an algorithm that is deemed to be less secure. This cost differential to the subscriber can be justified because of the direct correlation between the algorithm's sophistication, quality, and cost."

However this text does not disclose to one skilled in the art step (b) of the claimed invention. No part of Bhagavath addresses the cost other than the text quoted above. Furthermore, from a purely grammatical sense, the term "algorithm" is in the possessive tense. Thus, the sophistication, quality and cost refer to the sophistication, quality and cost of the algorithm itself, not the processing required to perform the algorithm.

Applicant points out that there is no technical reason within Bhagavath that would tie the price paid by the subscriber to the actual resources used to provide the desired security level. The value to the subscriber of the higher level of security need not have any relationship to the actual computational burden required to perform the cryptographic service. Nothing in Bhagavath teaches that there is a relationship between the level of security provided and the computational burden of providing that level of security.

Docket No.: A0461-US-NP

Application No.:09/569,924

Thus, original claim1 is not anticipated by Bhagavath. Original claim 8 is directed to a computer program that, when executed by a computer, causes the computer to perform the method of claim 1. Thus, claim 8 is not anticipated for the same reasons as original claim1 is not anticipated.

Original claim 15 is directed to a system that contains logic to perform the method of claim 1. Thus, claim 15 is not anticipated for the same reasons as original claim1 is not anticipated.

Thus, claims 1, 8, and 15 were improperly rejected under 35 U.S.C. 102(e) and applicant appeals to have this rejection reversed.

2. Claims 2, 9 and 16

Claims 2, 9, and 16 depend from and further limit their respective independent claims and thus are not anticipated. Thus, claims 2, 9, and 16 were improperly rejected under 35 U.S.C. 102(e) and applicant appeals to have this rejection reversed.

3. Claims 4, 11 and 18

Claims 4, 11, and 18 depend from and further limit their respective independent claims and thus are not anticipated. Thus, claims 4, 11, and 18 were improperly rejected under 35 U.S.C. 102(e) and applicant appeals to have this rejection reversed.

4. Claims 5, 12 and 19

Claims 5, 12, and 19 depend from and further limit their respective independent claims and thus are not anticipated.

In addition, and regarding the "Response to Arguments" paragraph of the final office action that starts with "On page 8,...", the Examiner again asserts that the "private information

Docket No.: A0461-US-NP

Application No.:09/569,924

retrieval” is retrieval of media services to subscribers of the cable system.” This reference is apparently to:

“Claims 5, 12 and 19 depend on and further limit their respective parent claims and thus are also not anticipated. Applicant respectfully points out that Bhagavath teaches absolutely nothing about Private Information Retrieval which would be understood by one skilled in the art at the time of the invention to mean technology that allows a user to retrieve a record of his/her choice from a database server such that nobody (not even the server) observes the identity of the record. Research on Private Information Retrieval was started around 1995.”

A “person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. This court explained that point well in *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1477 (Fed.Cir.1998):

It is the person of ordinary skill in the field of the invention through whose eyes the claims are construed. Such person is deemed to read the words used in the patent documents with an understanding of their meaning in the field, and to have knowledge of any special meaning and usage in the field. The inventor's words that are used to describe the invention--the inventor's lexicography--must be understood and interpreted by the court as they would be understood and interpreted by a person in that field of technology. Thus the court starts the decision making process by reviewing the same resources as would that person, viz., the patent specification and the prosecution history.” (*Phillips v. AWH Corporation*, *5, 2005 WL 1620331(Fed. Cir.(Colo.))).

Private Information Retrieval is discussed in the specification at page 22 line 4 through page 23, line 31. To summarize, Private Information Retrieval is technology that allows a user to retrieve a record of his/her choice from a database server such that nobody (not even the server) observes the identity of the record.

Bhagavath teaches absolutely nothing about Private Information Retrieval as that term is used within the specification at page 22 line 4 through page 23, line 31. Applicant believes that

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

the Examiner's assertion "that the 'private information retrieval' is retrieval of media services to subscribers of the cable system" has absolutely nothing to do with the instant application.

Thus, claims 5, 12, and 19 were improperly rejected under 35 U.S.C. 102(e) and applicant appeals to have this rejection reversed.

For these reasons, claims 1, 2, 4, 5, 8, 9, 11, 12, 15, 16, 18 and 19 were improperly rejected under 35 U.S.C. §102(e) as anticipated by Bhagavath et al (6,343,117 B1) and applicant respectfully requests reversal of this 35 U.S.C. §102(e) rejection.

Docket No.: A0461-US-NP

Application No.: 09/569,924

B. Whether claims 3, 10 and 17 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1 in view of Iwamura (6,272,535 B1)).

Applicant addresses the issue of non-obviousness of Claims 1, 8, and 15 with respect to Bhagavath to help advance the prosecution of the instant application towards allowance.

In rejecting claims under 35 U.S.C. §103(a), the Patent Office bears the initial burden of persuasion in establishing a prima facie case of obviousness. To achieve this, the Patent Office must show three criteria: a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine teachings; a reasonable expectation of success; and that the prior art must teach or suggest all claimed limitations. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See also MPEP §2143.

Having discussed the invention of claims 1, 8 and 15; and having discussed the teachings of Bhagavath; nothing in Bhagavath would have enabled one skilled in the art to make and use the method of claim 1, make and use the program product of claim 8 or make and use the system of claim 15.

The problem addressed by the invention of claims 1, 8, and 15 is that of identifying a computational burden required to perform a cryptographic service and determining a price for the cryptographic service based on the computational burden, privacy level, or speed.

The problem addressed by Bhagavath is that of encrypting data used in VoIP and of charging for that encryption based on the privacy level of the encryption. Nothing in Bhagavath suggests to one skilled in the art a modification to his technology to identify the computational burden required to perform the cryptographic service as Bhagavath's pricing is simply a function of the specified privacy level and not the computational burden required to provide the privacy level specified. Nothing in Bhagavath suggested the need for identifying a computational burden required to perform a cryptographic service.

Docket No.: A0461-US-NP

Application No.:09/569,924

Bhagavath does not address the problem addressed by the claimed invention. Bhagavath teaches techniques for allowing a user to select a desired security level where each of the security levels has a different price to the user.

Nothing in Bhagavath teaches identifying a computational burden required to perform the requested cryptographic service.

Furthermore, Bhagavath does not teach a suggestion, nor show a motivation that would enable one skilled in the art to make to identify such a computation burden.

Thus, claims 1, 8, and 15 are non-obvious over Bhagavath. Claims 2, 4, 5, 9, 11, 12, 16, 18, and 19 depend on and further limit, directly or indirectly, their respective independent claims that are patentable over Bhagavath. For at least this reason, claims 2, 4, 5, 9, 11, 12, 16, 18, and 19 are non-obvious over Bhagavath.

Turning now to Iwamura and claims 1 8, and 15.

1. **The asserted combination of references fails to teach the claimed invention.**

Iwamura teaches multiple ways to deliver and charge for providing information. The fourth embodiment teaches a user who specifies the level of encryption that is to be applied to the information prior to delivery and being charged accordingly. Iwamura does not teach a cryptographic service (as that term is used in the present application) but simply provides a mechanism for providing data that has been protected by a user-selected level of encryption. Iwamura also does not teach identifying a computational burden required to perform the cryptographic service.

Thus, Iwamura and Bhagavath separately or combined fail to teach the claimed invention.

Docket No.: A0461-US-NP

Application No.:09/569,924

2. **There is no motivation or suggestion in the prior art to make the asserted combination of references.**

The reason to make the asserted combination of references must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal Inc. v. F-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir. 1988), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. denied, 475 U.S. 1017 (1986); ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness.

Nothing in Bhagavath or Iwamura, separately or combined, motivate or suggest the combination for original claims 1, 8 and 15.

Thus, original claims 1, 8, and 15 are patentable over Bhagavath in view of Iwamura. In addition, original dependent claims 2, 4, 5, 9, 11, 12, 16, 18 and 19 that depend from and further limit their respective independent claims are also patentable.

With regards to claims 3, 10 and 17, these claims depend on and further limit their respective parent claims that are patentable. Thus claims 3, 10, and 17 are patentable.

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

C. Whether claims 6, 13 and 20 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1 in view of Billstrom (5,729,537)

The Bhagavath reference has been previously discussed with respect to independent claims 1, 8, and 15, and dependent claims 2, 4, 5, 9, 11, 12, 16, 18, and 19.

Billstrom teaches group authentication.

Nothing in Billstrom separately or combined with Bhagavath teaches a suggestion to one skilled in the art to identify a computational burden. Thus, original **claims 1, 8, and 15** are patentable over Bhagavath in view of Billstrom.

With regards to claims 6, 13, and 20 these claims depend on and further limit their respective parent claims that are patentable. Thus **claims 6, 13, and 20** are also patentable.

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

D. Whether claims 7, 14 and 21 are patentable under 35 U.S.C. §103(a) as being non-obvious over Bhagavath (6,343,117 B1 in view of Jakobsson (6,049,613 B1).

The Bhagavath reference has been previously discussed with respect to independent claims 1, 8, and 15, and dependent claims 2, 4, 5, 9, 11, 12, 16, 18, and 19.

Jakobsson teaches mix networks.

Nothing in Jakobsson separately or combined with Bhagavath teaches a suggestion to one skilled in the art to identify a computational burden. Thus, original **claims 1, 8, and 15** are patentable over Bhagavath in view of Jakobsson.

With regards to claims 7, 14, and 21 these claims depend on and further limit their respective parent claims that are patentable. Thus **claims 7, 14, and 21** are also patentable.

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

IX. Conclusion

For at least the reasons discussed above, it is respectfully submitted that claims 1-21 contain patentable subject matter and are distinguishable over the applied references.

Applicant respectfully requests the Honorable Board to reverse the final rejection of the claims and return the application to the Examiner to pass this case to issue.

Respectfully submitted,



Daniel B. Curtis
Attorney for Applicant(s)
Registration No. 39,159
Telephone: 650-812-4259

Date: July 25, 2005

Attachment: Appendix of Claims

Docket No.: A0461-US-NP

Application No.:09/569,924

X. Claims APPENDIX

1. (original): A method for pricing a cryptographic service, comprising:
 - (a) receiving a request for a cryptographic service;
 - (b) identifying a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing the cryptographic service; and
 - (c) determining a price of the cryptographic service based on the at least one of computational burden, privacy level, and speed.
2. (original): The method as recited in claim 1, wherein a user requesting the cryptographic service specifies the privacy level.
3. (original): The method as recited in claim 1, wherein a user requesting the cryptographic service specifies the speed of performing the cryptographic service.
4. (original): The method as recited in claim 1, further comprising requesting payment for the cryptographic service from a user requesting the cryptographic service.
5. (original): The method as recited in claim 1, wherein the cryptographic service includes utilizing private information retrieval.
6. (original): The method as recited in claim 1, wherein the cryptographic service includes utilizing group authentication.
7. (original): The method as recited in claim 1, wherein the cryptographic service includes utilizing mix networks.

Docket No.: A0461-US-NP

Application No.:09/569,924

8. (original): A computer program embodied on a compute readable medium for pricing a cryptographic service, comprising:
- (a) a code segment that receives a request for a cryptographic service;
 - (b) a code segment that identifies a computational burden required to perform the cryptographic service, including one or more of privacy level of the cryptographic service or speed of performing the cryptographic service; and
 - (c) a code segment that determines a price of the cryptographic service based on at least one of computational burden, privacy level, and speed.
9. (original): The computer program as recited in claim 8, wherein a user requesting the cryptographic service specifies the privacy level.
10. (original): The computer program as recited in claim 8, wherein a user requesting the cryptographic service specifies the speed of performing the cryptographic service.
11. (original): The computer program as recited in claim 8, further comprising a code segment that requests payment for the cryptographic service from a user requesting the cryptographic service.
12. (original): The computer program as recited in claim 8, wherein the cryptographic service includes utilizing private information retrieval.
13. The computer program as recited in claim 8, wherein the cryptographic service includes utilizing group authentication.
14. The computer program as recited in claim 8, wherein the cryptographic service includes utilizing mix networks.
15. (original): A system for pricing a cryptographic service, comprising:

Docket No.: A0461-US-NP

Application No.:09/569,924

- (a) logic that receives a request for a cryptographic service;
- (b) logic that identifies a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing the cryptographic service; and
- (c) logic that determines a price of the cryptographic service based on the at least one of the computational burden, privacy level, and speed.

16. (original): The system as recited in claim 15, wherein a user requesting the cryptographic service specifies the privacy level.
17. (original): The system as recited in claim 15, wherein a user requesting the cryptographic service specifies the speed of performing the cryptographic service.
18. (original): The system as recited in claim 15, further comprising logic that requests payment for the cryptographic service from a user requesting the cryptographic service.
19. (original): The system as recited in claim 15, wherein the cryptographic service includes utilizing private information retrieval.
20. (original): The system as recited in claim 15, wherein the cryptographic service includes utilizing group authentication.
21. (original): The system as recited in claim 15, wherein the cryptographic service includes utilizing mix networks.
22. (canceled):
23. (canceled):

Docket No.: **A0461-US-NP**

Application No.: **09/569,924**

24. (canceled):